A

ase type a plus (+) sign inside this box → [+]

65PTO/SB/05 REV 1 (12/97)
Approved for use through 09/30/2000. omb 0651-0032
Patent and Trademark Office: U S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

JC575 U.S. PTO 11/05/99

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1 53(b))

Attorney Docket No.	2189-20 LAM
First Inventor or Application Identifier:	RONALD C. MULLIN
Title	DIGITAL SIGNATURES ON A SMARTCARD
Express Mail Label No.	EL440665795US

JC675 U.S. PTO 09/434247 11/05/99

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, D C 20231

1. [X] Fee Transmittal Form
   (Submit an original, and a duplicate for fee processing)
2. [X] Specification [Total Pages 23]
   (preferred arrangement set forth below)
   - Descriptive title of the Invention
   - Cross References to Related Applications
   - Statement Regarding Fed sponsored R & D
   - Reference to Microfiche Appendix
   - Background of the Invention
   - Brief Summary of the Invention
   - Brief Description of the Drawings *(if filed)*
   - Detailed Description
   - Claim(s)
   - Abstract of the Disclosure
3. [X] Drawing(s) (35 USC) 113) [Total Sheets 7]
4. [X] Oath or Declaration [Total Pages 4]
   a. [X] Newly executed (original or copy)
   b. [ ] Copy from a prior application (37 CFR 1.63(d))
   (for continuation/divisional with Box 17 completed)
   [Note Box 5 below]
   i. [ ] DELETION OF INVENTOR(S)
   Signed statement attached in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
5. [ ] Incorporation by Reference *(useable if Box 4b is checked)*
   The entire disclosure of the prior application, from which a copy Of the oath or declaration is supplied under Box 4b, is considered As being part of the disclosure of the accompanying application And is hereby incorporated by reference therein.
6. [ ] Microfiche Computer Program *(Appendix)*
7. [ ] Nucleotide and/or Amino Acid Sequence Submission
   (if applicable, all necessary)
   a [ ] Computer Readable Copy
   b. [ ] Paper Copy (identical to computer copy)
   c. [ ] Statement Verifying identity

ACCOMPANYING APPLICATION PARTS

8. [X] Assignment Papers (cover sheet & document(s))
9. [ ] 37 CFR 3.73(b) Statement *(when there is an assignee)* [ ] Power of Attorney
10. [ ] English Translation Document (if applicable)
11. [X] Information Disclosure Statement (IDS)/PTO-1449 [ ] Copies of IDS Citations
12. [X] Preliminary Amendment
13. [X] Return Receipt Postcard (MPEP 503) *(Should be specifically itemized)*
14. [ ] Small Entity Statement(s) [ ] Statement filed in prior application, Status still proper and desired
15. [ ] Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
16. [X] Other: Check for $1,004.00

17. **If a CONTINUING APPLICATION,** *check appropriate box and supply the requisite information:*
[ ] Continuation [ ] Divisional [X] Continuation-in-part (CIP) of prior application No.: ____ / ____
Prior application information: *Examiner* ____ *Group/Art Unit* ____

18. **CORRESPONDENCE ADDRESS**

[ ] Customer Number or Bar Code Label ____ or [X] Correspondence address below
(Insert Customer No. or Attach bar code label here)

NAME	LAWRENCE A. MAXHAM
	BAKER & MAXHAM
ADDRESS	750 B STREET, SUITE 3100
	SYMPHONY TOWERS

CITY	SAN DIEGO	*STATE*	CALIFORNIA	*ZIP CODE*	92101
COUNTRY	USA	*TELEPHONE*	(619) 233-9004	*FAX*	(619) 544-1246

Name (Print/Type)	LAWRENCE A. MAXHAM	*Registration No. (Attorney/Agent)*	24,483
Signature	Lawrence A. Maxham	*Date*	5 NOVEMBER 1999

Practitioner's Docket No. 2189-20 *PATENT*

Preliminary Classification:

Proposed Class: 380
Subclass. 25

NOTE *"All applicants are requested to include a preliminary classification on newly filed patent applications The preliminary classification, preferably class and subclass designations, should be identified in the upper right-hand corner of the letter of transmittal accompanying the application papers, for example 'Proposed Class 2, subclass 129'" M P E P § 601 7th ed*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Box Patent Application
Assistant Commissioner for Patents
Washington, D.C. 20231

NEW APPLICATION TRANSMITTAL

Transmitted herewith for filing is the patent application of
inventor(s): Ronald C. Mullin, Scott A. Vanstone, Robert J. Lambert, Robert Gallant

WARNING: *37 C F R § 1 41(a)(1) points out*

"(a) A patent is applied for in the name or names of the actual inventor or inventors

"(1) The inventorship of a nonprovisional application is that inventorship set forth in the oath or declaration as prescribed by § 1 63, except as provided for in § 1 53(d)(4) and § 1 63(d) If an oath or declaration as prescribed by § 1 63 is not filed during the pendency of a nonprovisional application, the inventorship is that inventorship set forth in the application papers filed pursuant to § 1 53(b), unless a petition under this paragraph accompanied by the fee set forth in § 1 17(i) is filed supplying or changing the name or names of the inventor or inventors "

For (title): DIGITAL SIGNATURES ON A SMARTCARD

CERTIFICATION UNDER 37 C.F.R. § 1.10*
(Express Mail label number is mandatory)
(Express Mail certification is optional)

I hereby certify that this New Application Transmittal and the documents referred to as attached therein are being deposited with the United States Postal Service on this date 5 November 1999, in an envelope as "Express Mail Post Office to Addressee", mailing Label Number EL440665795US addressed to the Box Patent Application, Assistant Commissioner for Patents, Washington, D C. 20231.

John Dorsey
(type or print name of person certifying)

Signature of person mailing paper

WARNING: *Certificate of mailing (first class) or facsimile transmission procedures of 37 C F R § 1 8 cannot be used to obtain a date of mailing or transmission for this correspondence*

WARNING: *Each paper or fee filed by "Express Mail" must have the number of the "Express Mail" mailing label placed thereon prior to mailing 37 C F R § 1 10(b)*
"Since the filing of correspondence under § 1 10 without the Express Mail mailing label thereon is an oversight that can be avoided by the exercise of reasonable care, requests for waiver of this requirement will not be granted on petition " Notice of Oct 24, 1996, 60 Fed Reg 56,439, at 56,442

1. Type of Application

This new application is for a(n):

(check one applicable item below)

X Original (nonprovisional)

□ Design

□ Plant

WARNING: *Do not use this transmittal for a completion in the U.S. of an International Application under 35 U S C. § 371(c)(4), unless the International Application is being filed as a divisional, continuation or continuation-in-part application*

WARNING: *Do not use this transmittal for the filing of a provisional application.*

NOTE: *If one of the following 3 items apply, then complete and attach ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF A PRIOR U.S. APPLICATION CLAIMED and a NOTIFICATION IN PARENT APPLICATION OF THE FILING OF THIS CONTINUATION APPLICATION*

□ Divisional;

□ Continuation;

X Continuation-in-part (C-I-P).

2. Benefit of Prior U.S. Application(s) (35 U.S.C. §§ 119(e), 120, or 121)

NOTE *A nonprovisional application may claim an invention disclosed in one or more prior filed copending nonprovisional applications or copending international applications designating the United States of America In order for a nonprovisional application to claim the benefit of a prior filed copending nonprovisional application or copending international application designating the United States of America, each prior application must name as an inventor at least one inventor named in the later filed nonprovisional application and disclose the named inventor's invention claimed in at least one claim of the later filed nonprovisional application in the manner provided by the first paragraph of 35 U S C. § 112 Each prior application must also be*

(i) An international application entitled to a filing date in accordance with PCT Article 11 and designating the United States of America; or

(ii) Complete as set forth in § 1 51(b), or

(iii) Entitled to a filing date as set forth in § 1 53(b) or § 1 53(d) and include the basic filing fee set forth in § 1.16; or

(iv) Entitled to a filing date as set forth in § 1 53(b) and have paid therein the processing and retention fee set forth in § 1.21(l) within the time period set forth in § 1 53(f)

37 C F.R § 1.78(a)(1).

NOTE: *If the new application being transmitted is a divisional, continuation or a continuation-in-part of a parent case, or where the parent case is an International Application which designated the U S , or benefit of a prior provisional application is claimed, then check the following item and complete and attach ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U S. APPLICATION(S) CLAIMED.*

WARNING: *If an application claims the benefit of the filing date of an earlier filed application under 35 U S C. §§ 120, 121 or 365(c), the 20-year term of that application will be based upon the filing date of the earliest U.S. application that the application makes reference to under 35 U.S.C § 120, 121 or 365(c), (365 U.S C. § 154(a)(2) does not take into account, for the determination of the patent term, any application on which priority is claimed under 35 U S C. §§ 119, 365(a) or 365(b)) For a c-i-p application, applicant should review whether any claim in the patent that will issue is supported by an earlier application and, if not, the applicant should consider canceling the reference to the earlier filed application The term of a patent is not based on a claim-by-claim approach. See Notice of April 14, 1995, 60 Fed. Reg 20,195, at 20,205.*

WARNING: *When the last day of pendency of a provisional application falls on a Saturday, Sunday, or Federal holiday within the District of Columbia, any nonprovisional application claiming benefit of the provisional application must be filed prior to the Saturday, Sunday, or Federal holiday within the District of Columbia See 37 C F R § 1 78(a)(3)*

X The new application being transmitted claims the benefit of prior U.S. application(s). Enclosed are ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED.

3. Papers Enclosed

A. Required for filing date under 37 C.F.R. § 1.53(b) (Regular) or 37 C.F.R. § 1.153 (Design) Application

__15__ Pages of specification

__7__ Pages of claims

__7__ Sheets of drawing

WARNING *DO NOT submit original drawings A high quality copy of the drawings should be supplied when filing a patent application The drawings that are submitted to the Office must be on strong, white, smooth, and non-shiny paper and meet the standards according to § 1 84 If corrections to the drawings are necessary, they should be made to the original drawing and a high-quality copy of the corrected original drawing then submitted to the Office Only one copy is required or desired For comments on proposed then-new 37 C F R § 1 84, see Notice of March 9, 1988 (1990 O G 57-62)*

NOTE. *"identifying indicia, if provided, should include the application number or the title of the invention, inventor's name, docket number (if an y), and the name and telephone number of a person to call if the Office is unable to match the drawings to the proper application. This information should be placed on the back of each sheet of drawing a minimum distance of 1 5 cm (5/8 inch) down from the top of the page " 37 C F R § 1 84(c))*

(complete the following, if applicable)

□ The enclosed drawing(s) are photograph(s), and there is also attached a "PETITION TO ACCEPT PHOTOGRAPH(S) AS DRAWING(S)." 37 C.F.R. § 1.84(b).

X formal - Figs. 1 - 6

X informal – Figs. 7 - 9

B. Other Papers Enclosed

__4__ Pages of declaration and power of attorney

__1__ Pages of abstract

_____ Other

4. Additional Papers Enclosed

X Amendment to claims

X Cancel in this application **1 - 12** before calculating the filing fee. (At least one original independent claim must be retained for filing purposes.)

□ Add the claims shown on the attached amendment. (Claims added have been numbered consecutively following the highest numbered original claims).

X Preliminary Amendment

X Information Disclosure Statement (37 C.F.R. § 1.98)

X Form PTO-1449 (PTO/SB/08A and 08B)

□ Citations

- ☐ Declaration of Biological Deposit
- ☐ Submission of "Sequence Listing," computer readable copy and/or amendment pertaining thereto for biotechnology invention containing nucleotide and/or amino acid sequence
- ☐ Authorization of Attorney(s) to Accept and Follow Instructions from Representative.
- ☐ Special Comments
- ☐ Other

5. Declaration or oath (including power of attorney)

NOTE: A newly executed declaration is not required in a continuation or divisional application provided that the prior non-provisional application contained a declaration as required, the application being filed is by all or fewer than all the inventors named in the prior application, there is no new matter in the application being filed, and a copy of the executed declaration filed in the prior application (showing the signature or an indication thereon that it was signed) is submitted. The copy must be accompanied by a statement requesting deletion of the names of person(s) who are not inventors of the application being filed If the declaration in the prior application was filed under § 1 47, then a copy of that declaration must be filed accompanied by a copy of the decision granting § 1.47, then a copy of that declaration must be filed accompanied by a copy of the decision granting § 1 47 status or, if a nonsigning person under § 1.47 has subsequently joined in a prior application, then a copy of the subsequently executed declaration must be filed See 37 C F R §§ 1.63(d)(1)-(3)

NOTE A declaration to complete an application must be executed, identify the specification to which it is directed, identify each inventor by full name including family name and at least one given name, without abbreviation together with any other give name or initial, and the residence, post office address and country or citizenship of each inventor, and state whether the inventor is a sole or joint inventor 37 C.F.R § 1 63(a)(1)-(4)

X Enclosed

Executed by

(check all applicable boxes)

X inventor(s)

☐ legal representative of inventor(s) 37 C.F.R. §§ 1.42 or 1.43.

☐ joint inventor or person showing a proprietary interest on behalf of inventor who refused to sign or cannot be reached.

- ☐ This is the petition required by 37 C.F.R. § 1.47 and the statement required by 37 C.F.R. § 1.47 is also attached. See item 13 below for fee.

☐ Not Enclosed.

NOTE. Where the filing is a completion in the U.S. of an International Application or where the completion of the U S application contains subject matter in addition to the International Application, the application may be treated as a continuation or continuation-in-part, as the case may be, utilizing ADDED PAGE FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION CLAIMED.

☐ Application is made by a person authorized under 37 C.F.R.§ 1.41(c) on behalf of *all* the above named inventor(s).

(The declaration or oath, along with the surcharge required by 37 C.F.R. 1.16(e) can be filed subsequently)

□ Showing that the filing is authorized
(not required unless called question. 37 C.F.R. § 1.41(d))

6. Inventorship Statement

WARNING *If the named inventors are each not the inventors of all the claims an explanation, including the ownership of the various claims at the time the last claimed invention was made, should be submitted*

The inventorship for all the claims in this application are:

□ The same

or

X Not the same. An explanation, including the ownership of the various claims at the time the last claimed invention was made,

X is submitted

□ will be submitted

7. Language

NOTE An application including a signed oath or declaration may be filed in a language other than English An English translation of the non-English language application and the processing fee of $130 00 required by 37 C F R § 1 17(k) is required to be filed with the application, or within such time as may be set by the Office 37 C F R § 1 52(d)

X English

□ Non-English

□ The attached translation includes a statement that the translation is accurate. 37 C.F.R. § 1.52(d)

8. Assignment

X An assignment of the invention to Certicom Corp.

X is attached. A separate **X** "COVER SHEET FOR ASSIGNMENT (DOCUMENT) ACCOMPANYING NEW PATENT APPLICATION" or **X** FORM PTO-1595 is also attached.

□ will follow.

NOTE. "If an assignment is submitted with a new application, send two separate letters-one for the application and one for the assignment" Notice of May 4, 1`990 (1114 O G 77-78)

WARNING *A newly executed "CERTIFICATAE UNDER 37 C F R § 3 73(B)" must be filed when a continuation-in-part application is filed by an assignee Notice of April 30, 1993, 1150 O G 62-64*

9. Certified Copy

Certified copy(ies) of application(s)

Country	Appln No.	Filed
Country	Appln No.	Filed
Country	Appln No.	Filed

from which priority is claimed.

- ☐ is (are) attached.
- ☐ will follow

NOTE The foreign application forming the basis for the claim for priority must be referred to in the oath or declaration 37 C F R § 1 55(a) and 1 63

NOTE This item is for any foreign priority for which the application being filed directly relates If any parent U S application or International Application from which this application claims benefit under 35 U S C § 120 is itself entitled to priority from a prior foreign application, then complete item 18 on the ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U S APPLICATION(S) CLAIMED

10. Fee Calculation (37 C.F.R. § 1.16)

A. **X** Regular application

CLAIMS AS FILED

Number filed	Number Extra	Rate	Basic Fee 37 C F R § 1 16(a) $760 or $380
Total Claims (37 C F.R. § 1 16(c)	27 - 20=	7 XS18.00=	126
Independent Claims (37 C.F.R § 1.16(b))	4 - 3=	1 X$78 00=	78
Multiple dependent claim(s), if any (37 C.F.R § 1 16(d))	0 +	$260.00	0

X An amendment canceling extra claims is enclosed.

☐ An amendment deleting multiple-dependencies is enclosed.

☐ The fee for extra claims is not being paid at this time.

NOTE If the fees for extra claims are not paid on filing, they must be paid or the claims canceled by amendment, prior to the expiration of the time period set for response by the Patent and Trademark Office in any notice of fee deficiency 37 C F R § 1 16(d)

Filing Fee Calculation $ 964

B. ☐ Design application

($310.00—37 C.F.R. § 1.16(f))

Filing Fee Calculation $_____

C. ☐ Plant application

($480.00—37 C.F.R. § 1.16(g)

Filing Fee Calculation $_____

11. Small Entity Statement(s)

□ Statement(s) that this is a filing by a small entity under 37 C.F.R. §§ 1.9 and 1.27 is(are) attached.

WARNING: *"Status as a small entity must be specifically established in each application or patent in which the status is available and desired. Status as a small entity in one application or patent does not affect any other application or patent, including applications or patents which are directly or indirectly dependent upon the application or patent in which the status has been established. The refilling of an application under § 1.53 as a continuation, division, or continuation-in-part (including a continued prosecution application under § 1.53(d)), or the filing of a reissue application requires a new determination as to continued entitlement to small entity status for the continuing or reissue application. A nonprovisional application claiming benefit under 35 U.S.C. § 119(e), 120, 121, or 365© of a prior application, or a reissue application may rely on a statement filed in the prior application or in the patent if the nonprovisional application or the reissue application includes a reference to the statement in the prior application or in the patent or includes a copy of the statement in the prior application or in the patent and status as a small e ntity is still proper and desired. The payment of the small en tity baasic statutory filing fee will be treated as such a reference for purposes of this section." 37 C.F.R. § 1.28(a)(2).*

WARNING: *"Small entity status must not be established when the person or persons signing the . .statement can* ***unequivocally*** *make the required self-certification." M.P.E.P., § 509.03, 7th ed. (emphasis added).*

(complete the following, if applicable)

□ Status as a small entity was claimed in prior application _____/_____, filed on _____, from which benefit is being claimed for this application under:

35 U.S.C. § □ 119(e),
□ 120,
□ 121,
□ 365(c),

and which status as a small entity is still proper and desired.

□ A copy of the statement in the prior application is included.

Filing Fee Calculation (50% of A, B, or C above) $_____

NOTE: *Any excess of the full fee paid will be refunded if a small entity statement and a refund request are filed within 2 months of the date of timely payment of a full fee. The two-month period is not extendable under § 1.136. 37 C.F.R. § 1.28(a).*

13. Fee Payment Being Made at This Time

□ Not Enclosed

□ No filing fee is to be paid at this time
(This and the surcharge required by 37 C.F.R. § 1.6(e) can be paid subsequently.)

X Enclosed

X Filing fee $ 964

X Recording assignment
($40.00—37 C.F.R. § 1.21(h))
(See attached "COVER SHEET FOR ASSIGNMENT ACCOMPANYING NEW APPLICATION.") $ 40

□ Petition fee for filing by other than all the the inventors or person on behalf of the inventor where inventor refused to sign or cannot be reached
($130.00—37 C.F.R. §§ 1.47 and 1.17(i)) $_____

□ For processing an application with a specification in a non-English languague
($130.00—37 C.F.R. §§ 1.52(d) and 1.17(k)) $_____

□ Processing and retention fee
($130.00—37 C.F.R. §§ 1.53(d) and 1.21(l)) $_____

□ Fee for international-type search report
($40.00—37 C.F.R. §§ 1.21(e)) $_____

NOTE: 37 C.F.R. § 1.21(l) establishes a fee for processing and retaining any application that is abandoned for failing to complete the application pursuant to 37 C.F.R.§ 1.53(f) and this, as well as the changes to 37 C.F.R. §§ 1.53 and 1.78(a)(1), indicate that in order to obtain the benefit of a prior U.S. application, either the basic filing fee must be paid, or the processing and retention fee of § 1.21(L) must be paid, within 12 year from notification under § 53(f).

Total fees enclosed $ 1004

14. Method of Payment of Fees

X Check in the amount of $ 1004

□ Charge Account No._____ in the amount of $_____
A duplicate of this transmittal is attached.

NOTE: Fees should be itemized in such a manner that it is clear for which purpose the fees are paid. 37 C.F.R. §1.22(b).

15. Authorization to Charge Additional Fees

WARNING: *If no fees are to be paid on filing, the following items should not be completed.*

WARNING: *Accurately count claims, especially multiple dependent claims, to avoid unexpected high charges, if extra claim charges are authorized.*

X The Commissioner is hereby authorized to charge the following additional fees by this paper and during the entire pendency of this application to Account No. 02-0460

X 37 C.F.R. § 1.16(a), (f), or (g) (filing fees)

X 37 C.F.R. § 1.16(b), (c), or (d) (presentation of extra claims)

NOTE: *Because additional fees for excess or multiple dependent claims not paid on filing or on later presentation must only be paid or these claims canceled by amendment prior to the expired to the expiration of the time period set for response by the P.T.O. in any notice of fee deficiency (37 C.F.R. § 1.16(d)). It might be best not to authorize the P.T.O. to charge additional claim fees, except possibly when dealing with amendments after final action.*

□ 37 C.F.R. § 1.16(e) (surcharge for filing the basic filing fee and/or declaration on a date later than the filing date of the application)

□ 37 C.F.R. § 1.17(a)(1)-(5) (extension fees pursuant to § 1.136(a))

□ 37 C.F.R. § 1.17 (application processing fees)

NOTE: *". . . A written request may be submitted in an application that is an authorization to treat any concurrent or future reply, requiring a petition for an extension of time under this paragraph for its timely submission, as incorporating a petition for extension of time for the appropriate length of time. An authorization to charge all required fees, fees under § 1.17, or all required extension of time fees will be treated as a constructive petition for an extension of time in any concurrent or future reply requiring a petition for an extension of time under this paragraph for its timely submission. Submission of the fee set forth in § 1.17(a) will also be treated as a constructive petition for an extension of time in any concurrent reply requiring a petition for an extension of time under this paragraph for its timely submission." 37 C.F.R. § 1.135(a)(3).*

□ 37 C.F.R. § 1.18 (issue fee at or before mailing of Notice of Allowance, pursuant to 37 C.F.R. § 1.311(b))

NOTE: *Where an authorization to charge the issue fee to a deposit account has been filed before the mailing of a Notice of Allowance, the issue fee will be automatically charged to the deposit account at the time of mailing the Notice of Allowance. 37 C.F.R. § 1.311(b)).*

NOTE: *37 C.F.R. § 1.28(b) requires "Notification of any change in status resulting in loss of entitlement to small entity status must be filed in the application . . . prior to paying, or at the time of paying, . . . issue fee." From the wording of 37 C.FR. § 1.28(b), (a) notification of change of status must be made even if the fee is paid as "other than a small entity" and (b) no notification is required if the change is to another small entity.*

16. Authorization to Charge Additional Fees

NOTE. *" . . Amounts of twenty-five dollars or less will not be returned unless specifically requested within a reasonable time, nor will the payer be notified of such amounts, amounts over twenty-five dollars may be returned by check or, if requested, by credit to a deposit account " 37 C.F R. § 1 26(a)*

X Credit Account No. 02-0460

□ Refund

Date: 5 November 1999

SIGNATURE OF PRACTITIONER

Reg. No.: 24,483

Tel. No. (619) 233-9004

Lawrence A. Maxham
(type or print name of practitioner)

BAKER & MAXHAM
Symphony Towers, Suite 3100
705 "B" Street
San Diego, CA 92101

Customer No. 2189-20

X Incorporation by reference of added pages

(check the following item if the application in this transmittal claims the benefit of prior U.S. application(s) (including an international application entering the U.S. stage as a continuation, divisional or C-I-P application and complete and attch the ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED)

X Plus Added Pages for New Application Transmittal Where Benefit of Prior U.S. Application(s) Claimed

Number of pages added 5

X Plus Added Pages for Papers Referred to in Item 4 Above

Number of pages added 13

□ Plus added pages deleting names of inventor(s) named in prior application(s) who is/are no longer inventor(s) of the subject matter claimed in this application.

X Plus "Assignment Cover Letter Accompanying New Application"

Number of pages added 3

□ Statement Where No Further Pages Added

(if no further pages form a part of this Transmittal, then end this Transmittal with this page and check the following item)

□ This transmittal ends with this page.

Practitioner's Docket No. 2189-20 **PATENT**

ADDED PAGES FOR APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED

NOTE: See 37 C.F.R. § 1.78.

17. Relate Back

WARNING: *If an application claims the benefit of the filing date of an earlier filed application under 35 U.S.C. §§ 120, 121 or 365(c), the 20-year term of that application will be based upon the filing date of the earliest U.S. application that the application makes reference to under 35 U.S.C. §§ 120, 121 or 365(c). 35 U.S.C. § 154(a)(2) does not take into account, for the determination of the patent term, any application on which priority is claimed under 35 U.S.C. §§ 119, 365(a) or 365(b).) For a c-i-p application, applicant should review whether any claim in the patent that will issue is supported by an earlier application and, if not, the applicant should consider canceling the reference to the earlier filed application. The term of a patent is not based on a claim-by-claim approach. See Notice of April 14, 1995, 60 Fed. Reg. 20,195, at 20,205.*

(complete the following, if applicable)

☒ Amend the specification by inserting, before the first line, the following sentence:

A. 35 U.S.C. § 119(e)

NOTE: "Any nonprovisional application claiming the benefit of one or more prior filed copending provisional applications must contain or be amended to contain in the first sentence of the specification following the title a reference to each such prior provisional application, identifying it as a provisional application, and including the provisional application number (consisting of series code and serial number)." 37 C.F.R. § 1.78(a)(4).

☐ "This application claims the benefit of U.S. Provisional Application(s) No(s).:

APPLICATION NO(S).:	FILING DATE
_____ /_____	_____ "
_____ /_____	_____ "
_____ /_____	_____ "

B. 35 U.S.C. §§ 120, 121 and 365(c)

NOTE: "Except for a continued prosecution application filed under § 1.53(d), any nonprovisional application claiming the benefit of one or more prior filed copending nonprovisional applications or international applications designating the United States of America must contain or be amended to contain in the first sentence of the specification following the title a reference to each such prior application, identifying it by application number (consisting of the series code and serial number) or international application number and international filing date and indicating the relationship of the applications. . . . Cross-references to other related applications may be made when appropriate." (See § 1.14(a)). 37 C.F.R. § 1.78(a)(2).

☒ "This application is a

- ☐ continuation
- ☒ continuation-in-part
- ☐ divisional

of copending application(s)

☒ application number 08/632,845 filed on 4/16/96 "

☐ International Application _____ filed on

_____ and which designated the U.S."

NOTE: The proper reference to a prior filed PCT application that entered the U.S. national phase is the U.S. serial number and the filing date of the PCT application that designated the U.S.

NOTE: (1) Where the application being transmitted adds subject matter to the International Application, then the filing can be as a continuation-in-part or (2) if it is desired to do so for other reasons then the filing can be as a continuation.

NOTE: The deadline for entering the national phase in the U.S. for an international application was clarified in the Notice of April 26, 1987 (1079 O.G. 32 to 46) as follows:

"The Patent and Trademark Office considers the international application to be pending until the 22nd month from the priority date if the United States has been designated and no Demand for International Preliminary Examination has been filed prior to the expiration of the 19th month from the priority date and until the 32nd month from the priority date if a Demand for International Preliminary Examination which elected the United States of America has been filed prior to the expiration of the 19th month from the priority date, provided that a copy of the international application has been communicated to the Patent and Trademark Office within the 20 or 30 month period respectively. If a copy of the international application has not been communicated to the Patent and Trademark Office within the 20 or 30 month period respectively, the international application becomes abandoned as to the United States 20 or 30 months from the priority date respectivley. These periods have been placed in the rules as paragraph (h) of § 1.494 and paragraph (i) of § 1.495. A continuing application under 35 U.S.C. 365(c) and 120 may be filed anytime during the pendency of the international application."

☐ "The nonprovisional application designated above, namely application _____ / _____, filed _____, claims the benefit of U.S. Provisional Application(s) No(s).:

APPLICATION NO(S).:	FILING DATE
_____ / _____	_____ "
_____ / _____	_____ "
_____ / _____	_____ "

☐ Where more than one reference is made above, please combine all references into one sentence.

18. Relate Back—35 U.S.C. § 119 Priority Claim for Prior Application

The prior U.S. application(s), including any prior International Application designating the U.S., identified above in item 17B, in turn itself claim(s) foreign priority(ies) as follows:

Country	Appln. no.	Filed on

The certified copy(ies) has (have)

☐ been filed on _____, in prior application 0 /_____, which was filed on _____.

☐ is (are) attached.

WARNING: *The certified copy of the priority application that may have been communicated to the PTO by the International Bureau may not be relied on without any need to file a certified copy of the priority application* ***in the continuing application.*** *This is so because the certified copy of the priority application communicated by the International Bureau is placed in a folder and is not assigned a U.S. serial number unless the national stage is entered. Such folders are disposed of if the national stage is not entered. Therefore, such certified copies may not be available if needed later in the prosecution of a continuing application. An alternative would be to physically remove the priority documents from the folders and transfer them to the continuing application. The resources required to request transfer, retrieve the folders, make suitable record notations, transfer the certified copies, enter and make a record of such copies in the Continuing Application are substantial. Accordingly, the priority documents in folders of international applications that have not entered the national stage may not be relied on. Notice of April 28, 1987 (1079 O.G. 32 to 46).*

19. Maintenance of Copendency of Prior Application

NOTE: The PTO finds it useful if a copy of the petition filed in the prior application extending the term for response is filed with the papers constituting the filing of the continuation application. Notice of November 5, 1985 (1060 O.G. 27).

A. ☐ Extension of time in prior application

(This item ***must*** *be completed and the papers filed* ***in the prior application,*** *if the period set in the prior application has run.)*

☐ A petition, fee and response extends the term in the pending **prior** application until _____.

☐ A **copy** of the petition filed in prior application is attached.

B. ☐ Conditional Petition for Extension of Time in Prior Application

(complete this item, if previous item not applicable)

☐ A conditional petition for extension of time is being filed in the pending **prior** application.

☐ A **copy** of the conditional petition filed in the prior application is attached.

20. Further Inventorship Statement Where Benefit of Prior Application(s) Claimed

(complete applicable item (a), (b) and/or (c) below)

(a) ☐ This application discloses and claims only subject matter disclosed in the prior application whose particulars are set out above and the inventor(s) in this application are

- ☐ the same.
- ☐ less than those named in the prior application. It is requested that the following inventor(s) identified for the prior application be deleted:

(type name(s) of inventor(s) to be deleted)

(b) ☒ This application discloses and claims additional disclosure by amendment and a new declaration or oath is being filed. With respect to the prior application, the inventor(s) in this application are

- ☐ the same.
- ☒ the following additional inventor(s) have been added:

Robert J. Lambert and Robert Gallant

(type name(s) of inventor(s) to be added)

(c) The inventorship for all the claims in this application are

- ☐ the same.
- ☒ not the same. An explanation, including the ownership of the various claims at the time the last claimed invention was made
  - ☒ is submitted.
  - ☐ will be submitted.

New Figs. 7 - 9 have been added, together with revelant descriptive matter on pages 14 and 15 of the specification. New claims 28 - 39 have been added, necessitating the addition of inventors Lambert and Gallant. Ownership of all original and all new claims are and have been in the named assignee at all relevant times.

21. Abandonment of Prior Application *(if applicable)*

☐ Please abandon the prior application at a time while the prior application is pending, or when the petition for extension of time or to revive in that application is granted, and when this application is granted a filing date, so as to make this application copending with said prior application.

NOTE: According to the Notice of May 13, 1983 (103, TMOG 6-7), the filing of a continuation or continuation-in-part application is a proper response with respect to a petition for extension of time or a petition to revive and should include the express abandonment of the prior application conditioned upon the granting of the petition and the granting of a filing date to the continuing application.

22. Petition for Suspension of Prosecution for the Time Necessary to File an Amendment

WARNING: *"The claims of a new application may be finally rejected in the first Office action in those situations where (A) the new application is a continuing application of, or a substitute for, an earlier application, and (B) all the claims of the new application (1) are drawn to the same invention claimed in the earlier application, and (2) would have been properly finally rejected on the grounds of art of record in the next Office action if they had been entered in the earlier application." M.P.E.P., § 706.07(b), 7th ed.*

NOTE: Where it is possible that the claims on file will give rise to a first action final for this continuation application and for some reason an amendment cannot be filed promptly (e.g., experimental data is being gathered) it may be desirable to file a petition for suspension of prosecution for the time necessary.

(check the next item, if applicable)

☐ There is provided herewith a Petition To Suspend Prosecution for the Time Necessary to File An Amendment (New Application Filed Concurrently)

23. Small Entity (37 C.F.R. § 1.28(a))

☐ Applicant has established small entity status by the filing of a statement in parent application ____/_________ on __________ .

☐ A copy of the statement previously filed is included.

WARNING: *See 37 C.F.R. § 1.28(a).*

WARNING: *"Small entity status must not be established when the person or persons signing the . . . statement can **unequivocally** make the required self-certification." M.P.E.P., § 509.03, 7th ed. (emphasis added).*

24. NOTIFICATION IN PARENT APPLICATION OF THIS FILING

☒ A notification of the filing of this
(check one of the following)

☐ continuation
☒ continuation-in-part
☐ divisional

is being filed in the parent application, from which this application claims priority under 35 U.S.C. § 120.

ATTORNEY DOCKET NO.: 8700001-0205

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

In re patent application of:

RONALD C. MULLIN et al

Serial No.: Group Art Unit:

Filed: Examiner:

Title: Digital Signatures on a Smartcard

Assistant Commissioner for Patents
Washington, D.C. 20231

PRELIMINARY AMENDMENT

Sir:

IN THE CLAIMS

Cancel claims 1 to 12 submitted herewith

REMARKS

Claims 1 to 12 correspond in substance to claims 1 to 12 as allowed in the parent application 08/632,845 and are removed from consideration.

In the parent case, the Examiner considered the phrase "**in a deterministic but unpredictable manner**" recited in each independent claims 13 and 21 to be indefinite. The Examiner's position appeared to be that the terms "deterministic" and "unpredictable" are contradictory and therefore do not satisfy the requirements of 35 U.S.C. 112. To support that position the Examiner relied upon the extract from "Primality and Cryptography" by Kranakis, where it notes that for a pseudorandom sequence (which is deterministic), an exhaustive search could determine the seed from which the sequence was produced. This appears to be the basis for suggesting that such a deterministic generation cannot be unpredictable.

The Examiner failed to note that the same reference does, however, go on in the next sentence to note that such a search would be "of value *only if it were computationally feasible"* (emphasis added). In other words, although theoretically the seed can be obtained, in practice there are pseudorandom sequences for which the seed cannot be practically obtained. The section cited by the Examiner develops this theme, noting that certain generators are predictable and the development of general notions that emerge in subsequent sections include unpredictable pseudorandom generators. Given that a pseudorandom generator is deterministic as established by the passage relied on by the Examiner, the reference relied upon by the Examiner lends support for Applicants' use of the terminology" deterministic but unpredictable manner." In other words, this reference itself clearly suggests the existence of a device that operates in an "**unpredictable but deterministic manner.**"

The text "Applied Cryptography" by Bruce Schneier (ISBN 0-471-59756-2), at pages 39 through 41, discusses pseudorandom sequence generation i.e. in a deterministic manner and the concept of unpredictability. A copy of this section, together with face page of the book, is attached. From this section it would be noted that pseudorandom generators are deterministic in nature but within the general class of pseudorandom generation there are sub-classes that are suitable for cryptographic applications. A condition for a cryptographically random sequence is not only that it looks random but it must have the additional second property, namely, that it is *unpredictable.* The term "unpredictable" as applied in this art means "it must be computationally unfeasible to predict what the next random bit will be, given complete knowledge of the algorithms or hardware generating the sequence and all of the previous bits in the stream." Thus it may be seen that pseudorandom generators are deterministic, but they are also unpredictable if they satisfy the above requirement.

Quite clearly therefore within the context of cryptography there is a well established concept of operating in a deterministic but unpredictable manner and this is readily understood by those skilled in the particular art to which the present invention pertains.

The use of this concept is not restricted to the Schneier publication. Attached is an extract from a further publication by Kranakis namely "Theoretical Aspects of the Security of Public Key Cryptography" in which, at page 105, he makes reference to two security tests for

pseudorandom generators. The first one, the Blum-Mical test, is used to construct unpredictable pseudorandom generators. In other words, he is using terminology of a generator that operates in an unpredictable and pseudorandom or deterministic manner. Also enclosed is an extract from "Pseudorandomness and Crytographic Applications" by Michael Luby. At page 51, at Theorem 4.1, he defines a pseudorandom (deterministic) generator if and only if the generator is "next-bit unpredictable." Again the concepts of a deterministic operation with unpredictability are used.

It is submitted therefore that independent claims 13 and 21 to satisfy the requirements of 35 U.S.C. 112, second paragraph, in that they utilize language which is readily understood by a person skilled in the art to which the present invention pertains. The widespread use of that language has been demonstrated from a number of sources including the source relied upon by the Examiner and is therefore believed to provide a clear showing that the language of claims 13 and 21 is allowable. Further consideration to that end is respectfully requested. Claims 14-20 and 22-27 depend from and serve to further limit and define the invention of the independent claims.

Respectfully submitted,

______________________ Date

____
Lawrence A. Maxham
Attorney for the Applicant
Registration No. 24,483

DIGITAL SIGNATURES ON A SMARTCARD

This application is a continuation-in-part of Application 08/632,845.

The present invention relates to methods and apparatus for generating digital signatures.

It has become widely accepted to conduct transactions, such as financial transactions or exchange of documents, electronically. In order to verify the transaction, it is also well-known to "sign" the transaction digitally so that the authenticity of the transaction can be verified. The signature is performed according to a protocol that utilizes the message, i.e. the transaction, and a secret key associated with the party. The recipient can verify the signature using a public key of the signing party to recover the message and compare it with the transmitted message. Any attempt to tamper with the message or to use a key other than that of the signing party will result in an incompatibility between the sent message and that recovered from the signature or will fail to identify the party correctly and thereby lead to rejection of the transaction.

The signature must be performed such that the signing party's secret key cannot be determined. To avoid the complexity of distributing secret keys, it is convenient to utilize a public key encryption scheme in the generation of the signature. Such capabilities are available where the transaction is conducted between parties having access to relatively large computing resources but it is equally important to facilitate such transactions at an individual level where more limited computing resources are available.

Automated teller machines (ATMs) and credit cards are widely used for personal transactions and as their use expands, so the need to verify such transactions increases. Transaction cards, i.e. credit/debit cards or pass cards are now available with limited computing capacity (so-called "Smart Cards") but these do not have sufficient computing capacity to implement existing digital signature protocols in a commercially viable manner.

As noted above, in order to generate a digital signature, it is necessary to utilize a public key encryption scheme. Most public key schemes are based on the Diffie Helman Public key protocol and a particularly popular implementation is that known as DSS. The DSS scheme utilizes the set of integers Zp where p is a large prime. For adequate

security, p must be in the order of 512 bits although the resultant signature may be reduced mod q, where q divides p-1, and may be in the order of 160 bits.

The DSS protocol provides a signature composed of two components r, s. The protocol requires the selection of a secret random integer k referred to as the session key from the set of integers (0, 1, 2, . . . q-1), i.e.

$$k \in \{ 0, 1, 2, \ldots q-1 \}.$$

The component r is then computed such that

$$r = \{\beta^k \bmod p \} \bmod q$$

where β is a generator of q.

The component s is computed as

$$s = [k^{-1} (h(m)) + ar] \bmod q$$

where m is the message to be transmitted,

h(m) is a hash of that message, and

a is the private key of the user.

The signature associated with the message is then s,r which may be used to verify the origin of the message from the public key of the user.

The value β^k is computationally difficult for the DSS implementation as the exponentiation requires multiple multiplications mod p. This is beyond the capabilities of a "Smart Card" in a commercially acceptable time. Although the computation could be completed on the associated ATM, this would require the disclosure of the session key k to the ATM and therefore render the private key, a, vulnerable.

It has been proposed to precompute β^k and store sets of values of r and k on the card. The generation of the signature then only requires two 160 bit multiplications and signing can be completed within ½ second for typical applications. However, the number of sets of values stored limits the number of uses of the card before either reloading or replacement is required. A problem that exists therefore is how to generate sufficient sets of values within the storage and/or computing capacity of the card.

One possibility is to use a smaller value of p but with the DSS scheme this will jeopardize the security of the transaction.

An alternative encryption scheme that provides enhanced security at relatively small modulus is that utilizing elliptic curves in the finite field 2^m. A value of m in the order of 155 provides security comparable to a 512 bit modulus for DSS and therefore offers significant benefits in implementation.

Diffie Helman Public Key encryption utilizes the properties of discrete logs so that even if a generator β and the exponentiation β^k is known, the value of k cannot be determined. A similar property exists with elliptic curves where the addition of two points on a curve produces a third point on the curve. Similarly, multiplying any point on the curve by an integer k produces a further point on the curve. However, knowing the starting point and the end point does not reveal the value of the integer 'k' which may then be used as a session key for encryption. The value kP, where P is an initial known point, is therefore equivalent to the exponentiation β^k.

In order to perform a digital signature on an elliptic curve, it is necessary to have available the session key k and a value of kP referred to as a "session pair". Each signature utilizes a different session pair k and kP and although the representation of k and kP is relatively small compared with DSS implementations, the practical limits for "Smart Cards" are in the order of 32 signatures. This is not sufficient for commercial purposes.

One solution for both DSS and elliptic curve implementations is to store pairs of signing elements k, kP and combine stored pairs to produce a new session pair. For an elliptic curve application, this would yield a possible 500 session pairs from an initial group of 32 stored signing elements. The possibilities would be more limited when using DSS because of the smaller group of signing elements that could be stored.

In order to compute a new session pair, k and kP, from a pair of stored signing elements, it is necessary to add the values of k, e.g. $k_1 + k_2 \rightarrow k$ and the values of k_1P and k_2P to give a new value kP. In an elliptic curve, the addition of two points to provide a third point is performed according to set formula such that the addition of a point k_2P having coordinates (x,y) and a point k_1P having coordinates (x_2y_2) provides a point k_3P whose x coordinate x_3 is given by:

$$x_3 = \frac{y_1 \oplus y_2}{x_1 \oplus x_2}^2 \oplus \frac{y_1 \oplus y_2}{x_1 \oplus x_2} \oplus x_1 \oplus x_2.$$

This computation may be significantly simplified using the normal basis representation in a field $F2^m$, as set out more fully in our PCT Application Serial No. PCT /CA/900452, the contents of which are incorporated herein by reference. However, even using such advantageous techniques, it is still necessary to utilize a finite field multiplier and provide sufficient space for code to perform the computation. This is not feasible within the practical limits of available "Smart" cards.

As noted above, the ATM used in association with the card has sufficient computing power to perform the computation but the transfer of the coordinates of k_1P and k_2P from the card to the terminal would jeopardize the integrity of subsequent digital signatures as two of the stored signing elements would be known.

It is therefore an object of the present invention to obviate or mitigate the above disadvantages and facilitate the preparation of additional pairs of values from a previously stored set.

In general terms, one aspect of the present invention proposes to compute on one computing device an initial step in the computation of a coordinate of a point derived from a pair of points to inhibit recognition of the individual components, transfer such information to another computing device remote from said one device, perform at least such additional steps in said derivation at such other device to permit the completion of the derivation at said one device and transfer the result thereof to said one computing device.

Preferably, the initial step involves a simple field operation on the two sets of coordinates which provides information required in the subsequent steps of the derivation.

Preferably also the additional steps performed at the other device complete the derivation.

In a preferred embodiment, the initial step involves the addition of the x coordinates and the addition y coordinates to provide the terms $(x_1 \oplus x_2)$ and $(y_1 \oplus y_2)$.

The addition of the coordinates is an XOR operation that can readily be performed on the card and the results provided to the terminal.

In this manner, the coordinates (x,y) representing kP in a stored signing element are not disclosed as insufficient information is provided even with subsequent uses of the card. Accordingly, the x coordinate of up to 500 signatures can be generated from an initial set of 32 stored signing elements.

The new value of k can be computed on the card and to avoid computing the inverse k^{-1}, alternative known masking techniques can be utilized.

A further aspect of the present invention provides a method of generating additional sets of points from the initial set that may be used individually as a new value of kP or in combination to generate still further values of kP.

According to this aspect of the invention, the curve is an anomalous curve and the Frobenius Operator is applied to at least one of the coordinates representing a point in the initial set to provide a coordinate of a further point on the elliptic curve. The Frobenius Operator $\varnothing$ provides that for a point (x_1,y_1) on an anomalous curve, then $\varnothing (x_1,y_1)$ is a point (x_1^2,y_1^2) that also lies on the curve. In general, $\varnothing^i(x_1y_1)$ is a point x^{2^i}, y^{2^i} that also lies on the curve. For a curve over the field 2^m, there are m Frobenius Operators so for each value of kP stored in the initial set, m values of kP may be generated, referred to as "derived" values. The new value of k associated with each point can be derived from the initial relationship between P and $\varnothing$P and the initial value of k.

For a practical implementation where 32 pairs of signing elements are initially retained on the card and the curve is over the field 2^{155}, utilizing the Frobenius Operator provides in the order of 4960 possible derived values and by combining pairs of such derived values as above in the order of 10^7 values of kP can be obtained from the initial 32 stored signing elements and the corresponding values of k obtained to provide 10^7 session pairs.

Preferably, the stored values of kP are in a normal basis representation. The application Frobenius Operator then simply requires an "i" fold cyclic shift to obtain the value for an $\varnothing^i$ operation.

According to a further aspect of the invention, there is provided a method of generating signature components for use in a digital signature scheme, said signature components including private information and a public key derived from said private information, said method comprising the steps of storing private information and related public key as an element in a set of such information, cycling in a deterministic but

unpredictable fashion through said set to select at least one element of said set without repetition and utilizing said one element to derive a signature component in said digital signature scheme.

Embodiments of the invention will now be described by way of example only with reference to the accompanying drawings, in which

Figure 1 is a schematic representation of a programmable credit card;

Figure 2 is a schematic representation of a transaction performed between the card and network;

Figure 3 is a schematic representation of the derivation of a session pair from a pair of stored signing elements;

Figure 4 is a schematic representation of one step in the transmission of information shown in Figure 2;

Figure 5 is a schematic representation of a preferred implementation of the derivation of a session pair from two pairs of stored values; and

Figure 6 is a schematic representation of a selection unit shown in Figure 1.

Figure 7 is a schematic representation of a further embodiment of the derivation of session pairs from stored values.

The System

Referring therefore to Figure 1, a programmable credit card 10 (referred to as a 'SMART' card) has an integrated circuit 12 embedded within the body of card 10.

The integrated circuit includes a logic array 14, an addressable memory 16 and a communication bus 18. The memory 16 includes a RAM section 20 to store information, a pair of cyclic shift registers 22 for temporary storage of information and programming code 24 for control of the logic array 14 and communication bus 18. The array 14 includes an arithmetic unit 26 to provide modular arithmetic operation, e.g. additional and multiplication, and a selection unit 28 controlled by the programming code 24. It will be appreciated that the description of the card 10 is a schematic and restricted to that necessary for explanation of the preferred embodiment of the invention.

The card 10 is used in conjunction with a terminal 30, for example an automated teller machine (ATM), that is connected to a network to allow financial transactions to be conducted. The terminal 30 includes a keypad 32 to select options and

tasks and has computing capabilities to perform the necessary functions in conjunction with the card 10.

Access to the terminal 30 is obtained by inserting card 10 into a reader 34 and entering a pass code in a conventional manner. The pass code is verified with the card 10 through communication bus 18 and the terminal 30 activated. The keypad 32 is used to select a transaction, for example a transfer of funds, between accounts and generate a message through the network to give effect to the transactions, and card 10 is used to sign that transaction to indicate its authenticity. The signature and message are transmitted over the network to the intended recipient and upon receipt and verification, the transaction is completed.

The Card

The RAM section 20 of memory 16 includes digital data string representing a private key, a, which remains secret with the owner of the card and a corresponding public key Q = aP where P is the publicly known initial point on the selected curve. The RAM section 20 also includes a predetermined set of coordinates of points, kP, on an elliptic curve that has been preselected for use in a public key encryption scheme. It is preferred that the curve is over a finite field 2^m, conveniently, and by way of example only, 2^{155}, and that the points kP are represented in normal basis representation. The selected curve should be an anomalous curve, e.g. a curve that satisfies $y^2 + xy = x^3 + 1$, and has an order, e. Each point kP has an x coordinate and a y coordinate and is thus represented as two 155 digital data strings that are stored in the RAM 20. By way of example, it will be assumed that the RAM 20 contains 32 such points identified generically as kP and individually as k_0P, k_1P . . . $k_{31}P$. Similarly, their coordinates (x,y) will be individually designated x_0y_0 ... $x_{31}y_{31}$.

The points kP are precomputed from the chosen parameters of the curve and the coordinates of an originating point P. The k-fold addition of point P will provide a further point kP on the curve, represented by its coordinates (x,y) and the value of k cannot be determined even if the coordinates of points P and kP are known.

RAM 20 therefore contains the values of k associated with the respective points kP so that a set of stored signing elements k,kP is available for use in the signing of the transaction.

Signing

To sign a message m generated by the transaction, one session pair k_j; k_jP is required and may be obtained from RAM 20 as set out more fully below. Assuming that values k_j, k_jP have been obtained, the signing protocol requires a signature r,s) where

r is the data string representing the x-coordinate, x_j reduced mod q (q is a preselected publicly known divisor of e, the order of the curve, i.e. q/e_x);and

s $= [k^{-1}(h(m)) + ar] \bmod q$ where h(m) is a q-bit hash of the message m generated by the transaction.

In this signature, even though r is known, s contains the secret k and the private key, a, and so inhibits the extraction of either.

The generation of s requires the inversion of the value k and since k is itself to be derived from the stored set of values of k, it is impractical to store corresponding inverted values of possible k's. Accordingly, a known masking technique is used to generate components r, s^1 and u of a signature. This is done by selecting an integer, c, and computing a value u = ck. The value $s^{-1} = c(h(m) + ar) \bmod q$.

The signature value s can then be obtained by the recipient computing $s^1u^{-1} = k^{-1}[h(m) + ar]$.

The signature (r,s^1,u) can be computed on the card 10 and forwarded by bus 18 to the terminal 30 for attachment to the message m.

Generation of Session Pair

As noted above, in order to generate the signature (r,s), it is necessary to have for session pair k and kP. Security dictates that each session pair is only used once and it is assumed that the number of signing elements stored in RAM 20 is insufficient for commercial application.

In the preferred embodiment, two techniques are used to generate additional session pairs to the stored signing elements. It will be appreciated that each technique may be used individually although the combination of the two is preferred.

(i) Frobenius Operator

The first technique involves the use of the Frobenius Operator to derive additional session pairs from the stored signing elements and is shown in Figure 3. The Frobenius Operator denoted $\varnothing$ operates on a point P having coordinates (x,y) on an anomalous elliptic curve in the finite field 2^m such that $\varnothing^i P = (x^{2^i}, y^{2^i})$. Moreover, the point $\varnothing^i P$ is also on the curve. In the field 2^{155}, there are 155 Frobenius Operators so each point kP stored in memory 20 may generate 155 points on the curve by application of the Frobenius Operators. Thus, for the 32 values of kP stored, there are 4960 possible values of kP available by application of the Frobenius Operator.

To derive the value of $\varnothing^i P$, it is simply necessary to load the x and y coordinates of a point kP into respective shift registers 22 and perform an i-fold cyclic shift. Because the coordinates (x,y) have a normal basis representation, a cyclic shift in the register 22 will perform a squaring operation, and an i-fold cyclic shift will raise the value to the power 2^i. Therefore, after the application of i clock cycles, the registers 22 contain the coordinates of $\varnothing^i(kP)$ which is a point on the curve and may be used in the signing protocol. The 155 possible values of the coordinates (x,y) of $\varnothing^i(kP)$ may be obtained by simple cyclic shifting. The representations in the registers 22 may then be used to obtain r.

Where the use of Frobenius Operator provides sufficient values for commercial use, only one coordinate is needed to compute the value of r and so only a single shift register is needed. However, as will be described below, further session pairs can be derived if both the coordinates are known and so a pair of registers is provided.

For each value of $\varnothing^i(kP)$, it is necessary to obtain the corresponding value of k $\varnothing(P) = \lambda P$. λ is a constant that may be evaluated ahead of time and the values of its first m powers, λ^i computed. The m values are stored in RAM 20.

In general, $\varnothing^i(kP) \rightarrow \lambda^i kP$ so the value of k associated with $\varnothing^i(kP)$ is $\lambda^i k$. Since k is stored for each value of kP in RAM 20 and λ^i is also stored, the new value of k, i.e. $\lambda^i k$, can be computed using the arithmetic unit 26.

As an alternative, to facilitate efficient computation of λ^i and avoid excessive storage, it is possible to precompute specific powers of λ and store them in RAM 20. Because m is 155 in the specific example, the possible values of i can be represented as an 8-bit binary word. The values of $\lambda^2 \rightarrow \lambda^{2^7}$ are thus stored in RAM 20 and the value of λ represented in binary. The prestored values of λ^{2^1} are then retrieved as necessary and multiplied mod e by arithmetic unit 26 to provide the value of λ^1. This is then multiplied by k to obtain the new value associated with $\varnothing^i(kP)$.

It will be seen therefore that new session pairs k, kP may be derived simply and efficiently from the stored signing elements of the initial set. These session pairs may be computed in real time, thereby obviating the need to increase storage capacity and their computation utilizes simple arithmetic operations that may be implemented in arithmetic unit 26.

(ii) Combining Pairs

A further technique, illustrated schematically in Figure 4, to increase the number of session pairs of k and kP available, and thereby increase the number of signatures available from a card, is to combine pairs of stored signing elements to produce a new derived value. The addition of two points k_1P and k_2P will produce a third point k_3P that also lies on the curve and may therefore be used for signatures.

The addition of two points having coordinates $(x_1,y_1)(x_2y_2)$ respectively on a curve produces a new point having an x coordinate x_3 where

$$x_3 = \frac{y_1 \oplus y_2}{x_1 \oplus x_2}^2 \oplus \frac{y_1 \oplus y_2}{x_1 \oplus x_2} \oplus x_1 \oplus x_2$$

In the finite field 2m, y1⊕y2 and x1⊕x2 is an XOR field operation that may be performed simply in logic array 16. Thus the respective values of x_1 ,x_2 and y_1 ,y_2 are

placed in respective ones of registers 22 and XOR'd. The resultant data string is then passed over communication bus 16 to the terminal 30. The terminal 30 has sufficient computing capacity to perform the inversion, multiplication and summation to produce the value of x_3. This is then returned to register 22 for signature. The potential disclosure of x_3 does not jeopardize the security of the signature as the relevant portion is disclosed in the transmission of r.

The value of k_1+k_2 is obtained from the arithmetic unit 26 within logic array 16 to provide a value of k_3 and hence a new session pair k_3, k_3P is available for signature.

It will be appreciated that the value for y_3 has not been computed as the signing value r is derived from x_3 rather than both coordinates.

It will be noted that the values of x_1 and x_2 or y_1 and y_2 are not transmitted to terminal 30 and provided a different pair of points is used for each signature, then the values of the coordinates remains undisclosed.

At the same time, the arithmetic functions performed on the card are relatively simple and those computationally more difficult are performed on the terminal 30.

Preferred Implementation of Generating Session Pairs

The above technique may of course be used with pairs selected directly from the stored signing elements or with the derived values obtained using the Frobenius Operator as described above. Alternatively, the Frobenius Operator could be applied to the value of kP obtained from combining pairs of the stored signing elements to provide m possible values of each derived value.

To ensure security and avoid duplication of session pairs, it is preferred that only one of the stored signing elements should have the Frobenius Operator applied, as in the preferred embodiment illustrated in Figure 5.

In this arrangement, the coordinates x_1,y_1 of one of the stored signing elements is applied to the registers 22 and cyclically shifted i times to provide $\varnothing^i k_1P$.

The respective coordinates, $x_{\varnothing 1},y_{\varnothing 1}$, are XOR'd with the coordinates from another of the stored values k_2P and the summed coordinates transmitted to ATM 30 for computation of the coordinate x_3. This is retransmitted to the card 10 for computation of the value r.

The value of k_1 is processed by arithmetic unit 26 to provide $\lambda^j k$ and added to k_2 to provide the new value k_3 for generation of signature component s. In this embodiment, from an original set of 32 stored signing elements stored on card 10, it is possible to generate in the order of 10^7 session pairs. In practice, a limit of 10^6 is realistic.

Selection of Pairs Stored Signing Elements

The above procedure requires a pair of stored signing elements to be used to generate each session pair. In order to preserve the integrity of the system, the same set cannot be used more than once and the pairs of stored values constituting the set must not be selected in a predictable manner.

This selection function is performed by the selection unit 28 whose operation is shown schematically in Figure 6.

Selection unit 28 includes a set of counters 40,42,44 whose outputs address respective look up tables 46,48,50. The look up tables 46,48,50 map the successive outputs of the counters to pseudo random output values to provide unpredictability for the selection stored signing elements.

The 32 stored values of k and kP are assigned nominal designations as elements in a set 52 ranging from -15 to +15 with one designated ∞. To ensure that all available combinations of stored values are used without repetition, the nominal designations are grouped in 16 pairs in an ordered array 54 such that the difference (mod 31) in the assigned values of a pair uses all the numbers from 1 to 30. ∞ is grouped with 0. This array provides a first row of a notional matrix.

Successive rows 54a,b,c,etc. of the notional matrix are developed by adding 1 to each assigned designation of the preceding row until 15 rows are developed. In this way a matrix is developed without repetition of the designations in each cell. By convention $\infty + 1 = \infty$.

Counter 42 will have a full count after 15 increments and counter 40 will have a full count after 14 increments. Provided the full count values of counters 40,42 are relatively prime and the possible values of the counter 50 to select Frobenius Operator are relatively large, the output of counters 40,42,44 are mapped through the tables 46,48,50

respectively to provide values for row and column of the notional matrix and the order i of the Frobenius Operator to be applied.

The output of counter 48 selects a column of the array 54 from which a designation associated with a starting pair can be ascertained. In the example of Figure 6, the output of counter 42 is mapped by table 48 to provide an output of 3, indicating that column 3 of array 54 should be selected. Similarly, the output of counter 40 is mapped through table 46 to provide a count of 3 indicating that values in row 3 of the matrix should be used.

The assigned designations for a particular row are then obtained by adding the row value to the values of the starting pair. This gives a new pair of assigned designations that indicate the locations of elements in set 52. The signing elements are then retrieved from the set 52.

One of those pairs of signing elements is then output to a shift register 22 and operated upon by the designated Frobenius Operator ∅. The value of the Frobenius Operation is obtained from the output of table 50 which maps counter 44. The value obtained from table 5 sets the shift clock associated with register 22 so that the contents of the register 22 are cyclically shifted to the Frobenius value ∅ indicated by the output of table 50.

Accordingly, a new value for kP is obtained. The associated value of k can be computed as described above with the arithmetic unit utilizing the output of table 50 to determine the new value of λ. Accordingly, a derived value is obtained.

The derived value and signing element are then combined as described at (ii) above to provide a new session pair k, kP for use in the signing process.

The use of the counters 40,42 provides input values for the respective tables so that the array 54 is accessed in a deterministic but unpredictable fashion. The grouping of the pairs in the array 54 ensures there is no repetition in the selected elements to maintain the integrity of the signature scheme.

Counter 44 operates upon one of the selected pairs to modify it so that a different pair of values is presented for combination on each use, even though multiple access may be made to the array 54.

The counters 40,42,44 may also be utilized to limit the use of the Smart Card if desired so that a forced expiry will occur after a certain number of uses. Given the large number of possible signatures, this facility may be desirable.

Alternative structures to the look up tables 46,48,50 may be utilized, such as a linear feedback shift register, to achieve a mapped output if preferred.

Further selection of the session pairs can be obtained by preprocessing of the contents of register 52 using one or more of the techniques shown in Figures 7, 8 or 9.

In its simplest form, as shown in Figure 7, a source row 's' is selected and the session pair k_s,k_sP read from the register. A function is applied to the session pair, which for example is the Frobenius operation as set out in Figure 3 to provide a new session pair $\lambda^i k_s$; $\phi^i (k_s P)$. A destination row, d, is then selected in the table 52 and the new session pair combined with the contents of that row to generate a new pair of values. The contents of the table 52 are thus updated and a selection of pairs may be made for the generation of a new session pair as described above.

The preprocessing may be repeated a number of times with different source rows s, and destinations, d, so that a thorough mixing is obtained. The selection of source rows, s, and destinations, d, may be selected deterministically using the counters 40,42.

Alternatively, where the card 10 does not have adequate computing power or a curve other than an anomalous curve is used, an alternative function may be applied to the selected row. For example, a sign may be applied to the selected row prior to accumulation of a destination.

An alternative embodiment is shown in Figure 8 where multiple source rows $s_1 \ldots s_n$ are used and the selected session pairs combined. Typically two source rows are used but more than two can be combined if preferred. In this case the combining may proceed as shown in Figure 5 and the new value accumulated at the destination row, d, of the register. As the x coordinate of the combined point will identify one of the coordinates in the register 52, it is preferred to perform the computation on the card where feasible.

The selected session pairs may be modified prior to or subsequent to their addition by application of a second function, e.g. signing, (as shown in ghosted outline) to provide further security in the updating of the register 52.

Where a random number generator is incorporated on the card 10, the above preprocessing may be used effectively in the production of the cards. Referring to Figure 9, an initial set of session pairs is injected into the register 52 of each card 10. A random number generator 60 is run for an initial period and its output used to select the source and destination rows of the register 52. The source row is accumulated with the destination now so that the session pair of the set are changed with each iteration. If preferred, a function such as a sign or a Frobenius operation may be applied to the selected session pair before accumulation. The mixing continues for a further period with the output of generator 60 being used periodically to select each row. Once the register is considered thoroughly mixed, the session pairs may be selected and combined as described above for Figure 6. As the output of each generator 60 will vary from device to device, the sets of session pairs in each register 52 will also vary from device to device. Therefore the same initial table may be used but different session pairs will be generated.

In summary, therefore, pairs of signing elements from an initial set of stored values can be selected in a deterministic and unpredictable manner and one of those elements operated upon by the Frobenius Operator to provide additional values for the elements. The elements may then be combined to obtain a new session pair with a portion of the computation being performed off card but without disclosing the value of the elements. Accordingly, an extended group of session pairs is available for signing from a relatively small group of stored values.

We claim:

1. A method of generating a digital signature implemented over an elliptic curve public key encryption scheme utilizing information maintained secret in one computing device comprising the steps of

(i) initiating the computation of a coordinate a point on the elliptic curve from a pair of other points on said curve by performing on said one device an initial set of sufficient steps in the computation to inhibit recognition of information pertaining to the identity of said other points,

(ii) transferring to another computing device remote from the one device the results of said steps,

(iii) performing at least such additional steps in said computation at said other device to permit the completion of said computation at said one device, and

(iv) transferring the result of said additional steps to said one device for incorporation in said signature.

2. A method according to claim 1 wherein said initial steps includes a field operation to combine information from each of said other points.

3. A method according to claim 2 wherein said combined information is utilized in said additional steps.

4. A method according to claim 3 wherein said field operation includes the summation of the information representing one coordinate of each of said other points and the summation of the information representing the other coordinate of each of the other points.

5. A method according to claim 1 wherein said additional steps complete said computation.

6. A method according to claim 4 wherein said information representing the summation of said coordinates is transferred from said one device to said other device.

7. A method according to claim 4 wherein said elliptic curve is over the finite field 2^m and represents said coordinates in a normal basis in said field.

8. A method according to claim 7 wherein said additional steps includes cyclically shifting said information representing the summation of said coordinates.

9. A method according to claim 1 wherein said computation generates a single coordinate of said point, said single coordinates being utilized in said signing.

10. A method of deriving a coordinate of a point on an anomalous elliptic curve over the field $GF2^m$ for utilization in a public key encryption scheme implemented on said curve, said method comprising the steps of

(i) storing a normal basis representation of each of a set of coordinates of points on said curve,

(ii) retrieving said normal basis representation of a coordinate of one of said points;

(iii) performing an i-fold cyclic shift on said retrieved normal basis representation of said one coordinate, and

(iv) utilizing the resultant representation as a coordinate of a further point on the curve resulting from an i-fold application of the Frobenius Operator to said one point.

11. A method according to claim 10 wherein each of said set of coordinates represents a point on the curve that is an integer multiple k, of a starting point P, and the i-fold application of the Frobenius Operation to said staring point P produces a new point $\varnothing^i P$ where $\varnothing^i P = \lambda^i P$,

said method including the step of determining the integer k' associated with said further point by computing $k\lambda^i$.

12. A method of generating a session pair k,kP for use in a digital signature performed on an anomalous elliptic curve in the filed $GF2^m$ where kP is a point on said curve resulting from the k fold addition of a starting point P where k is an integer, said method comprising the steps of

(i) storing a set of initial values of k and kP, as a normal basis representation in the field $GF2^m$,

(ii) selecting a coordinate of one of said points kP in said set of initial values;

(iii) performing an i-fold cyclic shift on said coordinate to obtain a normal basis representation of the coordinate after an i-fold application of a Frobenius Operator;

(iv) selecting the integer k associated with said one of said points;

(v) computing an integer value $\lambda^i k$ where λ defines the relationship between the start point P and a point $\varnothing P$ and $\varnothing$ indicates a Frobenius Operation;

(vi) utilizing the resultant representation of the coordinate and the value $\lambda^i k$ as a session pair in a digital signature r,s where r is derived from the representation of a coordinate of a point on the curve and s is derived from the integer value associated with such point, the message to be signed and r.

13. A method of generating signature components for use in a digital signature scheme, said signature components including private information and a public key derived from said private information, said method comprising the steps of storing private information and related public key as an element in a set of such elements, cycling in a deterministic but unpredictable manner through said set to select at least one element of said set without repetition and utilizing said one element to derive a signature component in said digital signature scheme.

14. A method according to claim 13 wherein a pair of said elements are selected from said set and said pair of elements combined to provide said signature components.

15. A method according to claim 14 wherein one of said selected pair of elements is operated upon to produce private information and a public key derived from said one element prior to combination with the other of said elements.

16. A method according to claim 15 wherein a computation to combine said elements is initiated on one computing device and sufficient steps of said computation are performed on said one device to inhibit recognition of information in said elements and subsequent steps are performed on another computing device after transfer of a partially completed computation thereto.

17. A method according to claim 14 wherein said pairs of elements are selected by generating a pair of indices indicating respective locations of said elements in said set.

18. A method according to claim 17 wherein said indices are obtained from an ordered array arranged to provide each possible combination of indices.

19. A method according to claim 18 wherein said indices are selected from a counter that increments with each signature.

20. A method according to claim 19 wherein output from said counter is modified to provide a non-sequential selection of said indices.

21. A method of generating a digital signature implemented over an elliptic curve public key encryption scheme utilizing a session pair k, kP in which k is an integer maintained secret and kP represents a point on said curve resulting from a k-fold addition of starting point P, said method comprising the steps of storing a set of elements each having normal basis representation of a value of k and a normal basis representation of a value of kP in the field $GF2^m$, identifying each element of said set for subsequent retrieval, selecting a pair of said elements in a deterministic and unpredictable manner and combining said elements to provide a session pair for use in said digital signature.

22. A method according to claim 21wherein an auxiliary transformation is performed on one of said elements selected prior to combination with the other thereof.

23. A method according to claim 22 wherein said elliptic curve is an anomalous curve and said auxiliary transformation is an application of a Frobenius Operator.

24. A method according to claim 23 wherein said auxiliary transformation includes an i-fold cyclic shift on said normal basis representation of said value kP associated with said element.

25. A method according to claim 24 wherein said pairs of elements are selected from an ordered grouping of pairs of the identifications of said elements.

26. A method according to claim 22 wherein combining of said elements includes a computation performed in part on one computing device and in part on another computing device.

27. A method according to claim 26 wherein sufficient steps of said computation are performed on said one computing device to inhibit identification of either of said elements.

28. A method of generating a set of session pairs for use as a private key and a public key respectively in a public key cryptographic scheme, said method comprising the steps of establishing a set having a plurality of session pairs, selecting at least one of said session pairs, processing said selected session pair by applying a predetermined function thereto to generate a new session pair and incorporating said new session pair into said set.

29. A method according to claim 28 wherein said selection of said one of said session pairs is repeated a plurality of times.

30. A method according to claim 29 wherein a plurality of session pairs of said set is selected and combined to generate said new session pair.

31. A method according to claim 30 wherein said pairs are selected by a random number generator.

32. A method according to claim 31 wherein said selection of a plurality of pairs by said random number generator is repeated a plurality of times prior to said pairs being used to generate a private and public key pair.

33. A method according to claim 28 wherein said new session pairs are incorporated by accumulating said new session pair with an existing session pair.

34. A method according to claim 30 wherein an additional function is applied to at least one of said plurality of session pairs prior to combination with the other of said plurality of session pairs.

35. A method according to claim 30 wherein an additional function is applied after combination of said plurality session pairs to generate said new session pairs.

36. A method of generating a set of session pairs for use as a private key and a p7ublic key respectively in a public key cryptographic scheme, said method comprising the steps of establishing an initial set having a plurality of session pairs, selecting one of said pairs by a random selection process, and accumulating said selected pair with a randomly selected pair of said initial set.

37. A method according to claim 36 wherein successive selections and accumulations are performed on randomly selected ones of said set.

38. A method according to claim 37 wherein a function is applied to said selected one of said pairs prior to accumulation.

39. A method according to claim 37 wherein a random number generator is used to perform said random selections.

Abstract

A digital signature scheme for a "smart" card utilizes a set of prestored signing elements and combines pairs of the elements to produce a new session pair. The combination of the elements is performed partly on the card and partly on the associated transaction device so that the exchange of information between card and device does not disclose the identity of the signing elements. The signing elements are selected in a deterministic but unpredictable manner so that each pair of elements is used once. Further signing pairs are generated by implementing the signing over an anomalous elliptic curve encryption scheme and applying a Frobenius Operator to the normal basis representation of one of the elements.

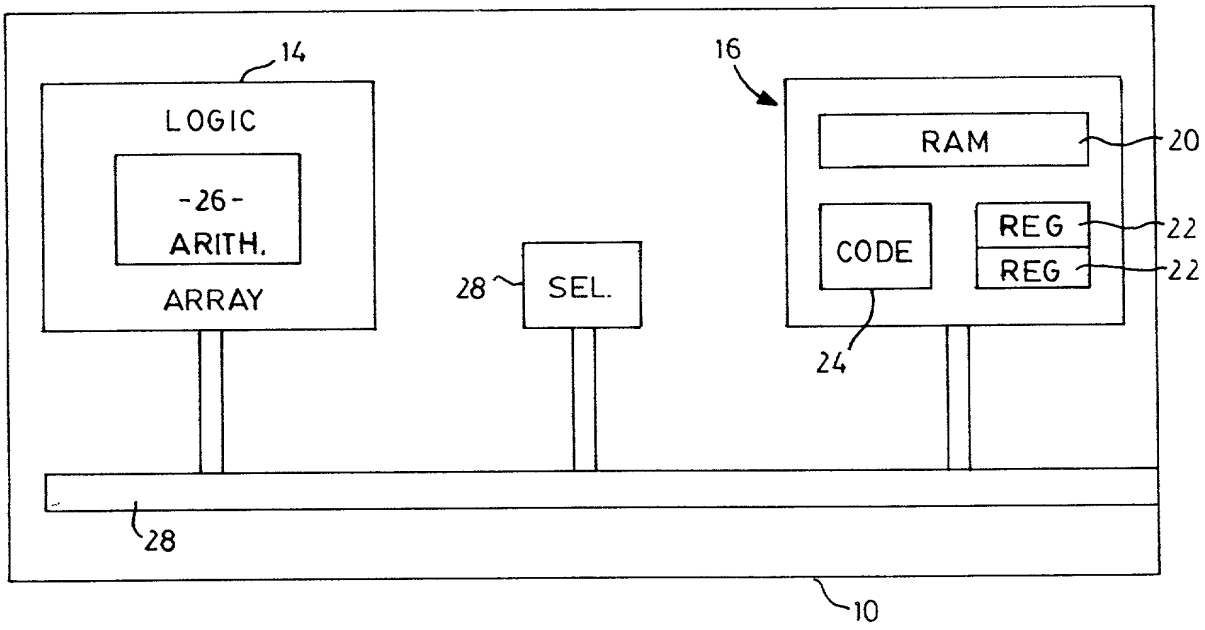
14
LOGIC
-26-
ARITH.
ARRAY
16
RAM
20
CODE
REG
22
REG
22
24
28
SEL.
28
10

FIG. 1

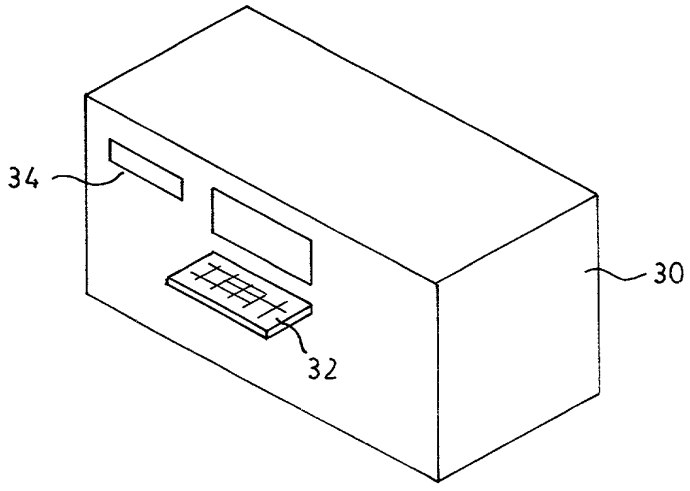
34
30
32

FIG. 2

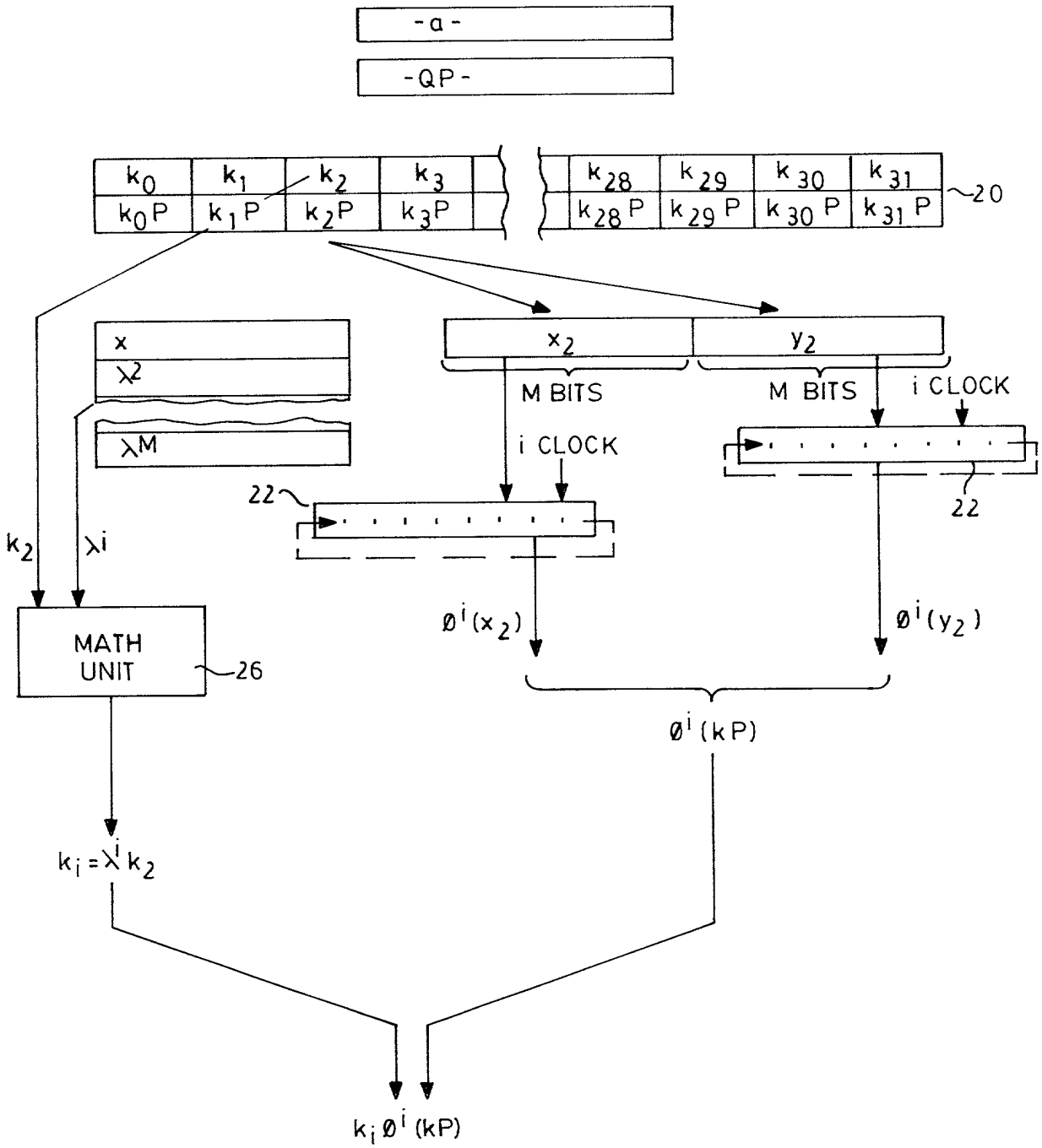
-a-
-QP-
k_0 k_1 k_2 k_3
k_0P k_1P k_2P k_3P
k_{28} k_{29} k_{30} k_{31}
$k_{28}P$ $k_{29}P$ $k_{30}P$ $k_{31}P$
20
x
λ^2
λ^M
x_2
y_2
M BITS
M BITS
i CLOCK
i CLOCK
22
22
k_2
λi
MATH UNIT
26
$\phi^i(x_2)$
$\phi^i(y_2)$
$\phi^i(kP)$
$k_i = \lambda^i k_2$
$k_i \phi^i(kP)$

FIG. 3

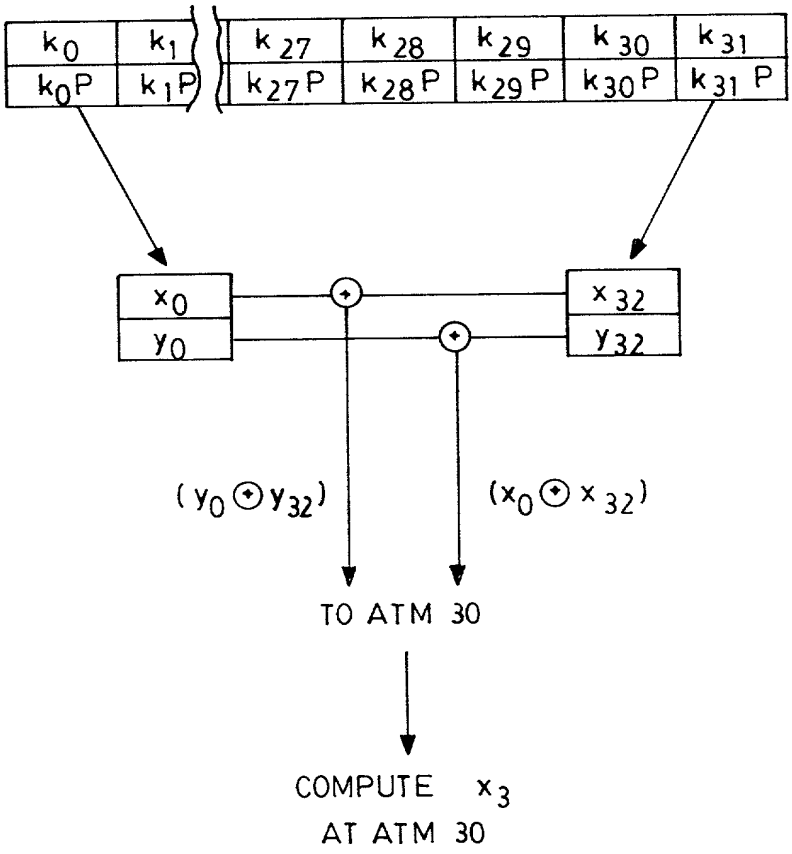
k_0
k_1
k_{27}
k_{28}
k_{29}
k_{30}
k_{31}
k_0P
k_1P
$k_{27}P$
$k_{28}P$
$k_{29}P$
$k_{30}P$
$k_{31}P$
x_0
y_0
x_{32}
y_{32}
$(y_0 \oplus y_{32})$
$(x_0 \oplus x_{32})$
TO ATM 30
COMPUTE x_3
AT ATM 30

FIG. 4

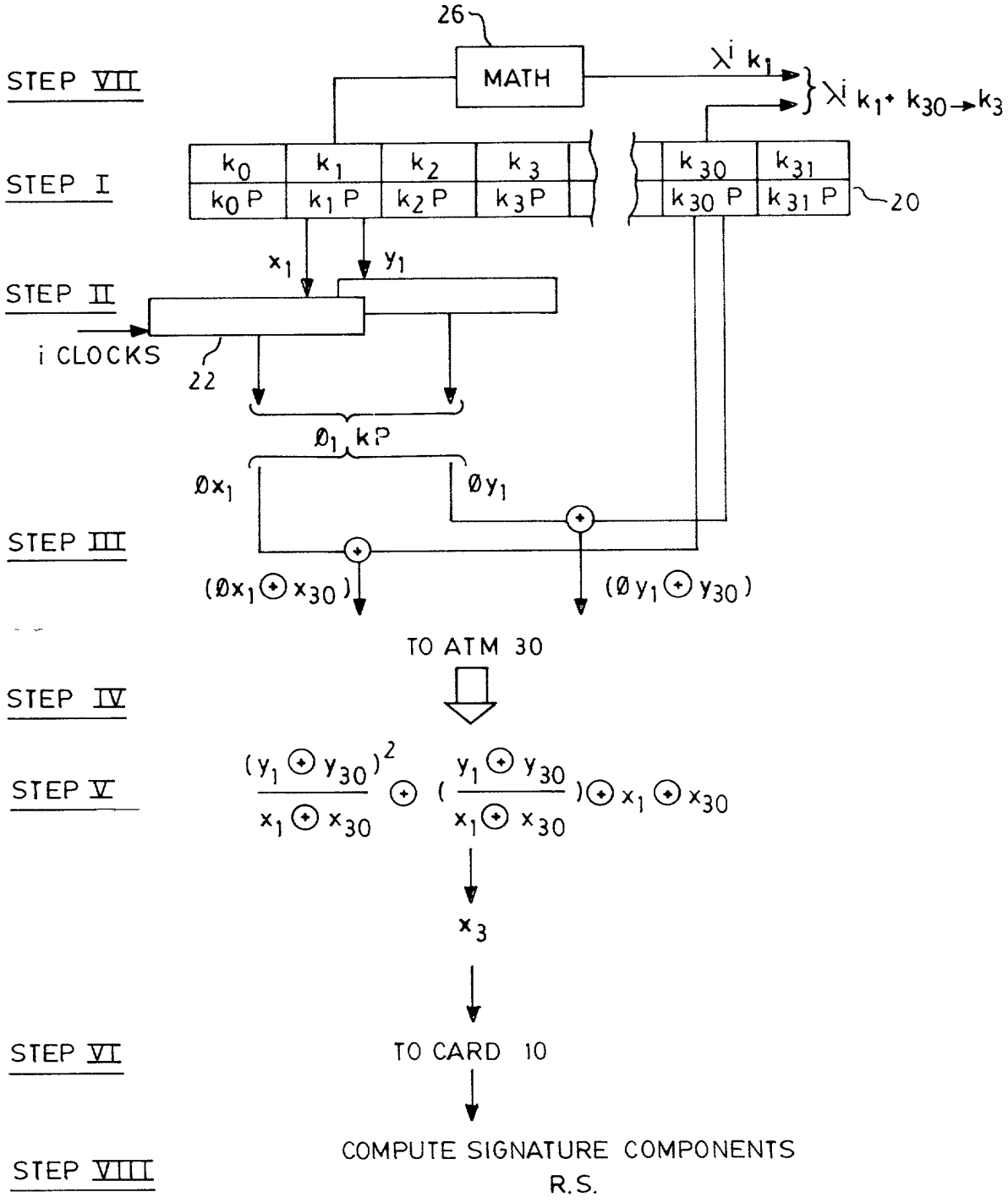
26
MATH
STEP VII
$\lambda^i k_1$
$\lambda^i k_1 + k_{30} \rightarrow k_3$
STEP I
k_0 k_1 k_2 k_3
$k_0 P$ $k_1 P$ $k_2 P$ $k_3 P$
k_{30} k_{31}
$k_{30} P$ $k_{31} P$
20
x_1
y_1
STEP II
i CLOCKS
22
$\emptyset_1 kP$
STEP III
$\emptyset x_1$
$\emptyset y_1$
$(\emptyset x_1 \oplus x_{30})$
$(\emptyset y_1 \oplus y_{30})$
TO ATM 30
STEP IV
STEP V
$\frac{(y_1 \oplus y_{30})^2}{x_1 \oplus x_{30}} \oplus (\frac{y_1 \oplus y_{30}}{x_1 \oplus x_{30}}) \oplus x_1 \oplus x_{30}$
x_3
STEP VI
TO CARD 10
STEP VIII
COMPUTE SIGNATURE COMPONENTS
R.S.

FIG. 5

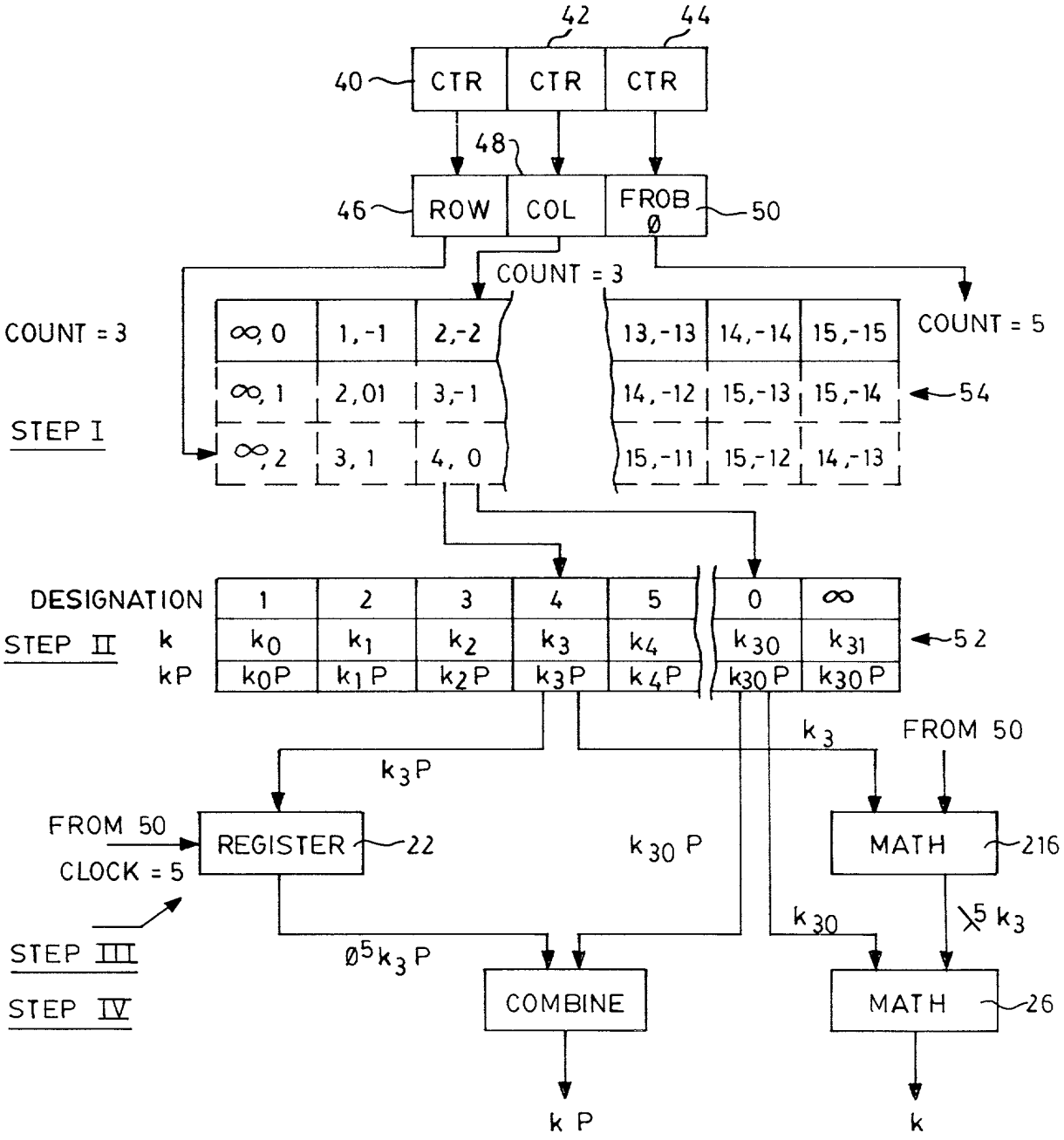
42
44
40
CTR
CTR
CTR
48
46
ROW
COL
FROB
Ø
50
COUNT = 3
COUNT = 3
COUNT = 5
∞, 0
1, -1
2, -2
13, -13
14, -14
15, -15
∞, 1
2, 01
3, -1
14, -12
15, -13
15, -14
54
STEP I
∞, 2
3, 1
4, 0
15, -11
15, -12
14, -13
DESIGNATION
1
2
3
4
5
0
∞
STEP II
k
k0
k1
k2
k3
k4
k30
k31
52
kP
k0P
k1P
k2P
k3P
k4P
k30P
k30P
k3
FROM 50
k3P
FROM 50
REGISTER
22
k30 P
MATH
216
CLOCK = 5
k30
5 k3
STEP III
Ø5k3P
COMBINE
MATH
26
STEP IV
k P
k

FIG. 6

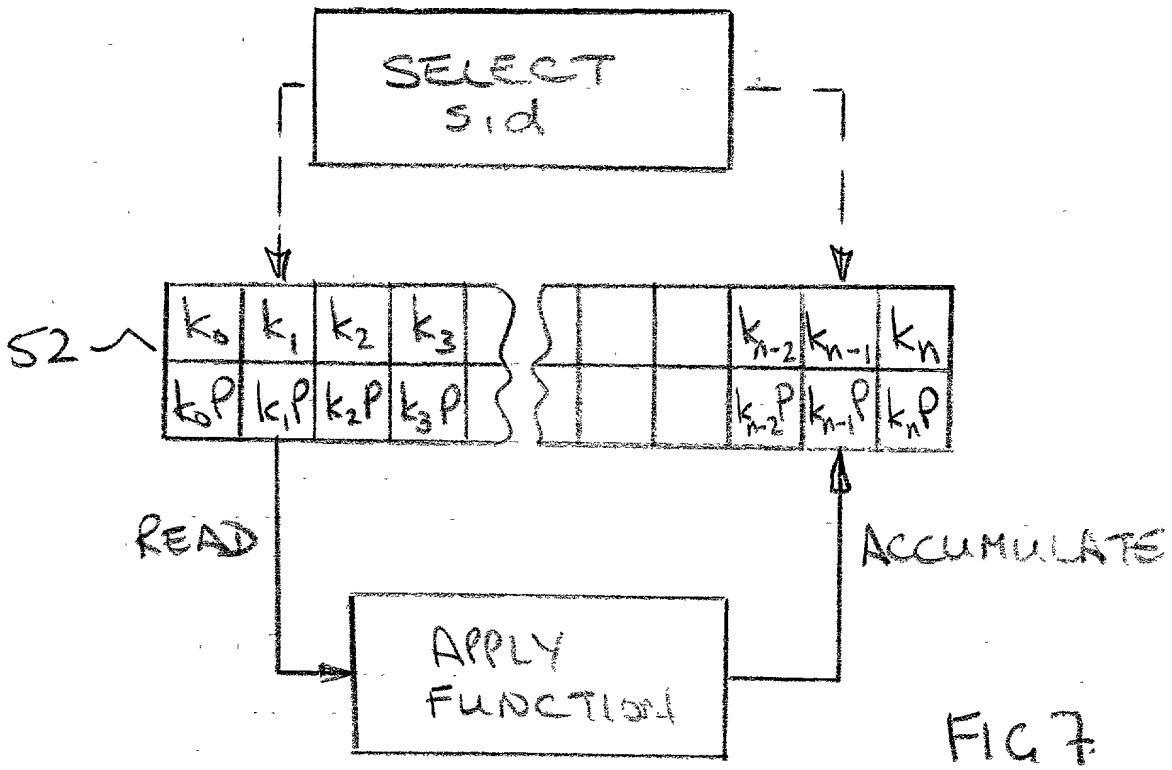
SELECT
s, d
S2
READ
ACCUMULATE
APPLY
FUNCTION

FIG 7.

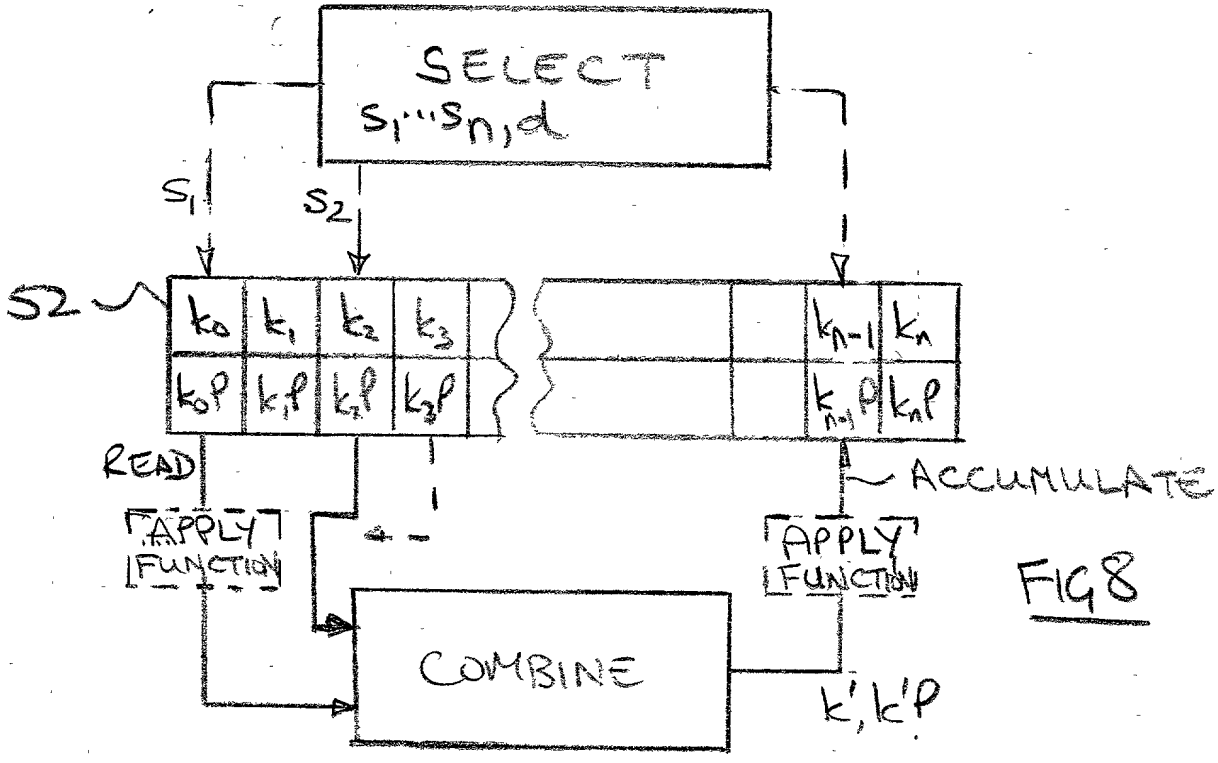
SELECT
$s_1 \cdots s_n, d$
s_1
s_2
S2
READ
ACCUMULATE
APPLY
FUNCTION
APPLY
FUNCTION
COMBINE
k', k'P

FIG 8

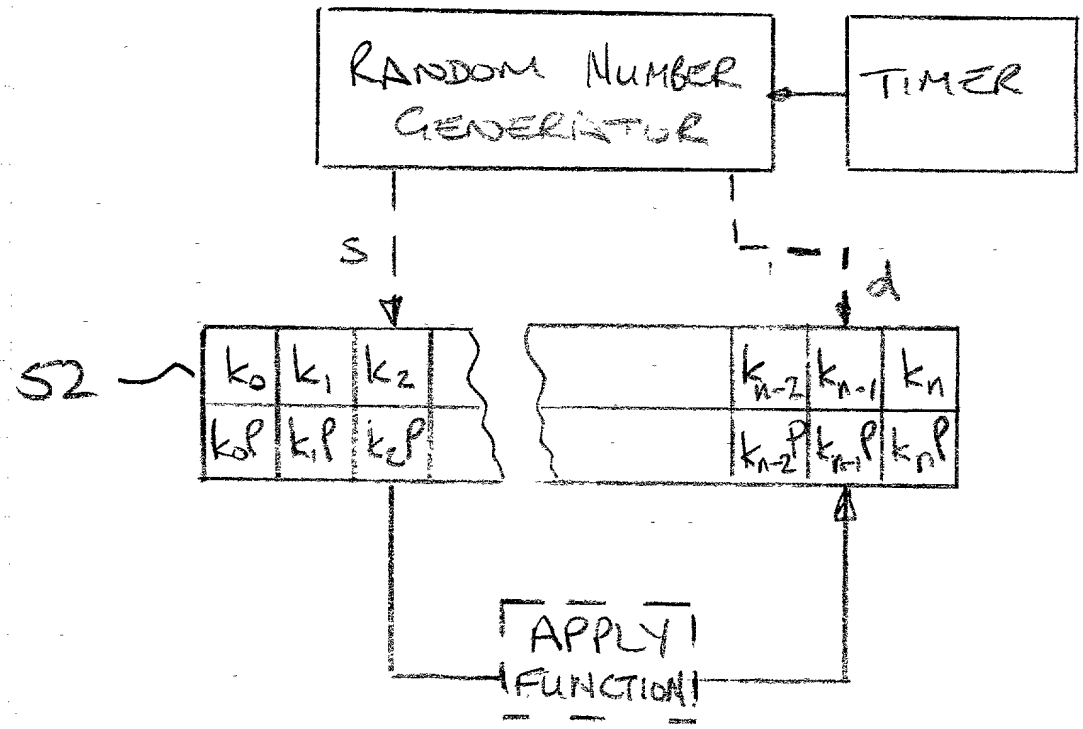
RANDOM NUMBER GENERATOR
TIMER
S
d
52
k_0 k_1 k_2
k_0P k_1P k_2P
k_{n-2} k_{n-1} k_n
$k_{n-2}P$ $k_{n-1}P$ k_nP
APPLY FUNCTION

FIG 9

Docket No.
8700001-0205

Declaration and Power of Attorney For Patent Application

English Language Declaration

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

Digital Signatures on a Smartcard
Continuation of U.S. Patent Application 08/632,845

the specification of which

(check one)

☒ is attached hereto.

☐ was filed on _____ as United States Application No. or PCT International Application Number _____

and was amended on _____
(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d) or Section 365(b) of any foreign application(s) for patent or inventor's certificate, or Section 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate or PCT International application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)			Priority Not Claimed
_____ (Number)	_____ (Country)	_____ (Day/Month/Year Filed)	☐
_____ (Number)	_____ (Country)	_____ (Day/Month/Year Filed)	☐
_____ (Number)	_____ (Country)	_____ (Day/Month/Year Filed)	☐

I hereby claim the benefit under 35 U.S.C. Section 119(e) of any United States provisional application(s) listed below:

(Application Serial No.)	(Filing Date)
(Application Serial No.)	(Filing Date)
(Application Serial No.)	(Filing Date)

I hereby claim the benefit under 35 U. S. C. Section 120 of any United States application(s), or Section 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. Section 112, I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, C. F. R., Section 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application:

(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)
08/632,845	**April 16, 1996**	**Pending**

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. *(list name and registration number)*

Lawrence A. Maxham **24,483**

Send Correspondence to: **Lawrence A. Maxham**
Baker & Maxham
Symphony towers, 750 'B' Street
Suite 3100, San Diego, CA 92101 U.S.A.

Direct Telephone Calls to: *(name and telephone number)*
Lawrence A. Maxham Telephone - (619) 233-9004 Facsimile - (619) 544-1246

Full name of sole or first inventor **Ronald C. Mullin**
Sole or first inventor's signature R C Mullin Date Oct 12, 1999
Residence **533 Twin Oaks Crescent**
Citizenship **Canadian**
Post Office Address **Waterloo, Ontario N2L 4R9 Canada**

Full name of second inventor, if any **Scott A. Vanstone**
Second inventor's signature S A Vanstone Date October 12, 1999
Residence **10140 Pineview Trail**
Citizenship **Canadian**
Post Office Address **Campbellville, Ontario, Canada**

Full name of third inventor, if any
Robert J. Lambert

Third inventor's signature

Date
October 12 1999

Residence
63 Holm Street

Citizenship
Canadian

Post Office Address
Cambridge, Ontario N3C 3N3, Canada

Full name of fourth inventor, if any
Rob Gallant

Fourth inventor's signature

Date
October 12 1999

Residence
4788 ROSEBUSH ROAD

Citizenship
CANADIAN

Post Office Address
MISSISSAUGA, ONTARIO, L5M 5N1, CANADA

Full name of fifth inventor, if any

Fifth inventor's signature

Date

Residence

Citizenship

Post Office Address

Full name of sixth inventor, if any

Sixth inventor's signature

Date

Residence

Citizenship

Post Office Address